UNTIED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

SHANDRELLE HARPER, and DANIEL FRANK, individually, and on behalf of all others similarly situated, Plaintiffs, v. COMCAST CABLE COMMUNICATIONS LLC d/b/a XFINITY; CITRIX SYSTEMS INC., Defendants.	2:24-cv-00072-RMG **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiffs Shandrelle Harper and Daniel Frank (collectively "Plaintiffs"), individually and on behalf of all others similarly situated, allege the following against Comcast Cable Communications LLC d/b/a Xfinity ("Xfinity") and Citrix Systems Inc. ("Citrix") (collectively, "Defendants"):

NATURE OF THE ACTION

1. Plaintiffs bring this class action lawsuit due to Defendants' failure to properly secure and safeguard sensitive and confidential personally identifiable information ("PII")[1], including account usernames, passwords, the last four digits of Social Security numbers, account security questions, birthdates, and contact information of many of its current customers.

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal oridentifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

Defendants' wrongful disclosure has harmed Plaintiffs and the Classes (defined below), which include millions of people.

2. This data breach is estimated to affect 35.8 million people.[2] Many of these people now have their account information accessible by cybercriminals and will be more likely to be victims of cyber-attacks and potential scams.

3. Defendants knew or should have known that due the increasing number of well-publicized data breaches that have occurred in the United States, large data storage such as this require the highest level of protection, which Defendant failed to provide.

4. Plaintiffs and members of the Class ("Class Members") entrusted Xfinity with their sensitive and valuable Personal Information. Plaintiffs and Class Members did not know that Defendants' data security was inadequate. They did not expect that services offered by Defendants would directly cause such serious injuries that would last for years after the service.

5. Defendants have caused harm to Plaintiffs and Class Members by collecting, using, and maintaining their Personal Information for its own economic benefit but utterly failing to protect that information. Defendants did not maintain adequate security systems, did not properly archive Personal Information, allowed access by third parties, and did not implement sufficient security measures.

JURISDICTION AND VENUE

6. This Court possesses subject-matter jurisdiction to adjudicate the claims set forth herein under the provisions of the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and

[2] https://www.cbsnews.com/news/xfinity-hack-customers-usernames-passwords/ (last accessed January 3, 2024).

costs, (2) the action is a class action, (3) there are members of the Class, including Plaintiffs, who are citizens of States diverse from Defendants, and (4) there are more than 100 Class Members.

7. This Court has Personal Jurisdiction over Defendants because Defendants have sufficient minimal contacts with this District. Defendants have purposefully availed themselves to this Jurisdiction through their marketing, sale, advertising, and promotion of its products, services, and retail stores throughout this Jurisdiction.

8. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391 because Defendants transact their business in this District, and a substantial part of the events and/or omissions giving rise to the claims occurred, in part, within this District.

PARTIES

PLAINTIFFS

9. Plaintiff Shandrelle Harper is a resident of Charleston County, South Carolina.

10. Prior to the data breach, Plaintiff Harper had been a loyal Xfinity customer since 2015.

11. On December 20, 2023, Plaintiff Harper received notice from Xfinity that her personal data had been exposed in Defendants' data breach.

12. Plaintiff Harper has been careful to protect her PII that was exposed in the Defendants' data breach.

13. Even with the precautions, Plaintiff Harper has had her identity compromised and been forced to file an identity theft report with the Federal Trade Commission.

14. Plaintiff Harper will continue to be at a higher risk of cyber-attacks, as well as the target of spam and scams for the foreseeable future because of Defendants' breach.

15. Plaintiff Daniel Frank is a resident of Gwinnett County, Georgia.

16. Plaintiff Frank is currently, and has been an Xfinity customer for years.

17. On December 29, 2023, Plaintiff Frank received an email notice from Xfinity that his personal data had been exposed in Defendants' data breach.

18. Now that his data has been accessed by cybercriminals, Plaintiff Frank will be at a higher risk of cyber-attacks, as well as the target of spam and scams for the foreseeable future because of Defendants' breach.

DEFENDANTS

19. Defendant Comcast Cable Communications LLC d/b/a Xfinity is a global media and technology company, producing and distributing entertainment, sports, and news worldwide.[3]

20. Defendant Xfinity provides broadband, mobile, and entertainment services on a subscription basis to millions of customers.[4]

21. Defendant Xfinity is headquartered in Pennsylvania, with its principal place of business located at Comcast Center, 1701 John F. Kennedy Blvd; Philadelphia, PA 19103.

22. Defendant Citrix Systems Inc. is a cloud computing and virtualization technology company. The Company develops server, application and desktop virtualization, networking, software as a service, cloud computing, and digital workspace solutions. Citrix Systems serves over 16 million customers worldwide.[5]

23. Defendant Citrix is headquartered in Fort Lauderdale, Florida, with its principal place of business located at 851 Cypress Creek Road Fort Lauderdale, FL 33309.

[3] https://corporate.comcast.com/company (last accessed January 3, 2024).
[4] *Id.*
[5] https://www.citrix.com/ (last accessed January 3, 2024);
https://www.bloomberg.com/profile/company/CTXS:US (last accessed January 3, 2024).

24. Defendant Xfinity relies on Defendant Citrix's cloud computing services for Xfinity's business operations.

FACTUAL ALLEGATIONS

25. On October 10, 2023, Citrix released information relating to the Citrix Bleed vulnerability (CVE-2023-4966) ("Citrix Bleed") which affects Netscaler Gateway and Netscaler ADC products. It allows threat actors to exploit and bypass password requirements and multi-factor authentication to hijack legitimate user sessions and acquire elevated permissions to harvest credentials and access data and resources.

26. On the same day, Citrix released security updates to patch the Citrix Bleed, to strengthen the security of the Citrix systems and prevent unauthorized actors from continuing to gain access.

27. Xfinity failed to timely install the patch, and on October 25, 2023, Xfinity discovered suspicious activity and subsequently determined that between October 16 and 19, unauthorized access to its internal systems occurred.[6] Six days after Citrix made the Citrix Bleed public and released a software patch.

28. By failing to properly manage their vulnerability and install the proactive patch, Xfinity has inadvertently allowed unauthorized users access to millions of customer's personal data, putting them at higher risk of being the target of a cyber-attack and victims of identity fraud and other scams.

29. Upon information and belief, the Personal Information stolen in the Data Breach included account usernames, passwords, multi-factor authentication codes, the last four digits of

[6] https://www.malwarebytes.com/blog/news/2023/12/comcasts-xfinity-breached-by-citrix-bleed-36-million-customers-data-accessed (last accessed January 3, 2024).

Social Security numbers, account security questions, birthdates, and contact information of many of its current customers.

30. Because of Defendants' Data Breach, Plaintiffs will continue in perpetuity to invest, time and money into additional precautionary and monitoring measures that could, but may not successfully, mitigate the potential misuse of their data.

31. The Data Breach was the product of an intentional criminal act to gain access to the data. It was the result of a sophisticated, intentional, and malicious attack by professional cybercriminal hackers and was not the result of an accidental disclosure by an Xfinity or Citrix employee. Thus, the risk that the victims will experience identity theft or fraud is much more real.

32. As a result of the Data Breach, Plaintiffs and members of the Class must be more vigilant of phishing emails and spam telephone calls. Such scams trick consumers into giving more information and other valuable personal information to scammers. This significantly increases the risk of further substantial damages to Plaintiffs and the Class, including, but not limited to, monetary and identity theft.

CLASS ACTION ALLEGATIONS

33. Plaintiffs bring this action on behalf of themselves, and all others similarly situated pursuant to Rule 23(a) and Rule 23 (b)(3) of the Federal Rules of Civil Procedure. Plaintiffs seek class certification on behalf of the class defined as follows ("the Class").

> **Nationwide Class:** All persons in the United States who were customers of Comcast Cable Communications LLC d/b/a Xfinity during the time of October 16 through 19 2023.

34. Excluded from the Class are any Defendants, any parent companies, subsidiaries, and/or affiliates, officers, directors, legal representatives, employees, co-conspirators, all governmental entities, and any judge, justice or judicial officer presiding over this matter.

35. The Nationwide Class shall be referred to as the "Class." Proposed Members of said Class will be referred to as "Class Members," or otherwise referenced as "members of the Class."

36. **Numerosity:** The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiffs are informed and believe that the proposed Class contains millions of customers who have been damaged by Defendants' conduct as alleged herein. The precise number of Class Members is estimated to be 35.8 million.

37. **Typicality:** Plaintiffs' claims are typical to those of all Class Members because members of the Class are similarly injured through Defendants' uniform misconduct described above and were subject to their personal data released due to Defendants' conduct. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all members of the Class.

38. **Commonality:** Plaintiffs' claims raise questions of law and fact common to all members of the Class, and they predominate over any questions affecting only individual Class Members. The claims of Plaintiffs and all prospective Class Members involve the same alleged data breach. These common legal and factual questions include the following:

a. Whether Defendants' data breach exposed their personal information

b. Whether Defendants owed a duty of care to Plaintiffs and the Class;

c. Whether Defendants knew or should have known that their data security was inadequate;

d. Whether Defendants wrongfully represent, and continue to represent, that their security is adequate;

e. Whether the alleged conduct constitutes violations of the laws asserted;

f. Whether Defendants' alleged conduct violates public policy;

g. Whether Defendants' representations in advertising are false, deceptive, and misleading;

h. Whether a reasonable consumer would consider the risk of their data being exposed when choosing to do business with Defendants;

i. Whether Defendants breached their express warranties;

j. Whether Defendants breached their implied warranties;

k. Whether certification of any or all of the classes proposed herein is appropriate under Fed. R. Civ. P. 23; and

l. Whether Plaintiffs and the Class Members are entitled to damages and/or restitution and the proper measure of that loss.

39. **Adequacy:** Plaintiffs and their counsel will fairly and adequately protect and represent the interests of each member of the Class. Plaintiffs have retained counsel experienced in complex litigation and class actions. Plaintiffs' counsel has successfully litigated other class action cases similar to that here and has the resources and abilities to fully litigate and protect the interests of the Class. Plaintiffs intends to prosecute this claim vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class, nor are Plaintiffs subject to any unique defenses.

40. **Superiority:** A class action is superior to the other available methods for a fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by Plaintiffs and the individual Class Members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendants. It would thus be virtually impossible for Plaintiffs and Class Members, on an individual basis, to obtain meaningful and effective redress for the wrongs done to them. Further, it is desirable to concentrate

the litigation of the Class Members' claims in one forum, as it will conserve party and judicial resources and facilitate the consistency of adjudications. Plaintiffs know of no difficulty that would be encountered in the management of this case that would preclude its maintenance as a class action.

41. The Class also may be certified because Defendants have acted or refused to act on grounds applicable to the Class, thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

42. Plaintiffs seek preliminary and permanent injunctive and equitable relief on behalf of the entire Class, on grounds generally applicable to the entire Class, to enjoin and prevent Defendants from continuing to provide inadequate data security. Further, Plaintiffs seek for Defendants to provide a full refund all protective and defensive procedures that Plaintiffs and the Class Members have had to employ.

43. Unless a Class is certified, Plaintiffs and the Class Members will continue to be injured due to Defendants' conduct. Unless a Class-wide injunction is issued, Defendants may continue to commit the violations alleged and the members of the Class and future customers may continue to be placed in harms' way.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

44. Plaintiffs incorporate Paragraphs 1-43 by reference as if fully set forth herein.

45. As part of the regular course of its business operations Defendants gathered and stored the PII of Plaintiffs and Class Members. Plaintiffs and the Class were entirely dependent on

Defendants to use reasonable measures to safeguard their PII and were vulnerable to the foreseeable harm of a security breach should Defendants fail to safeguard their PII.

46. By collecting and storing this data in its computer property, and sharing it, and using it for commercial gain, Defendants assumed a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it— to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

47. Defendants owed a duty of care to Plaintiffs and the Class to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

48. Defendants' duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as Defendants'. Various FTC publications and data security breach orders further form the basis of Defendants' duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

49. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

50. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses,

which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

51. Defendants gathered and stored the PII of Plaintiffs and the Class as part of their business of soliciting its services to its customers which solicitations and services affect commerce.

52. Defendants violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiffs and Class Members and by not complying with applicable industry standards.

53. Defendants breached their duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard their PII, and by failing to provide prompt notice without reasonable delay.

54. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and its customers, which is recognized by laws and regulations including but not limited to FTCA, as well as common law. Defendants were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and the Class or minimize the Data Breach.

55. Defendants' multiple failures to comply with applicable laws and regulations, and the violation of Section of 5 of the FTC Act constitutes negligence *per se*.

56. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

57. Defendants had full knowledge of the sensitivity of the PII, the types of harm that Plaintiffs could and would suffer if the PII was wrongfully disclosed, and the importance of adequate security.

58. Plaintiffs and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class had no ability to protect their PII that was in Defendants' possession.

59. Defendants were in a special relationship with Plaintiffs and the Class with respect to the hacked PII because the aim of Defendant's data security measures was to benefit Plaintiffs by ensuring that their PII would remain protected and secure. Only Defendants were able to ensure that their systems were sufficiently secure to protect Plaintiffs' and other Class Members' PII. The harm to Plaintiffs and the Class from its exposure was highly foreseeable to Defendants.

60. Defendants owed Plaintiffs and other Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing their PII, including acting to reasonably safeguard such data and providing notification to Plaintiffs and the Class of any breach in a timely manner so that appropriate action could be taken to minimize losses.

61. Defendants had duties to protect and safeguard the PII of Plaintiffs and other Class Members from being vulnerable to compromise by taking common-sense precautions when dealing with highly sensitive PII. Additional duties that Defendants owed Plaintiffs and the Class include:

a. Exercising reasonable care in designing, implementing, maintaining, monitoring, and testing Defendants' networks, systems, protocols, policies, procedures, and practices to ensure that individuals PII was adequately secured from impermissible release, disclosure, and publication;
b. To protect Plaintiffs' and the Class's PII in its possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiffs and the Class of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their PII.

62. Only Defendants were in a position to ensure that their systems and protocols were sufficient to protect the PII that had been entrusted to them.

63. Defendants breached their duties of care by failing to adequately protect Plaintiffs' and the Class's PII. Defendants breached their duties by:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the PII in its possession;
b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;
c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;
d. Failing to adequately train its employees to not store unencrypted PII in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;
e. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's PII;
f. Failing to mitigate the harm caused to Plaintiffs and the Class;
g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and
h. Failing to promptly notify Plaintiffs and other Class Members of the Data Breach that affected their PII.

64. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

65. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Class during the time the PII was within Defendants' possession or control.

66. Defendants' failure to provide timely and clear notification of the Data Breach to Plaintiffs and the Class prevented Plaintiffs and the Class from taking meaningful, proactive steps to securing their PII and mitigating damages.

67. Defendants' wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

68. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; and (viii) future costs in terms of time, effort, and money

that will be expended to monitor bank accounts and credit reports, prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and members of the Class.

69. As a direct and proximate result of Defendants' negligence, Plaintiffs, and members of the Class have suffered (and will continue to suffer) other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non- economic losses.

70. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and members of the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

71. Plaintiffs and members of the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

72. Plaintiffs and the Class seek actual damages, attorney's fees, costs, and any other just and proper relief available thereunder for Defendants' negligent handling of their PII.

COUNT II
BREACH OF CONTRACT
(On Behalf of Plaintiffs and the Class)

73. Plaintiffs incorporate Paragraphs 1-43 by reference as if fully set forth herein.

74. As part of doing business with Defendants, Plaintiffs and members of the Class are required to provide Defendants with personal information when entering a contract with Defendant Xfinity before they are able to receive the benefit of any services from Defendants.

75. All Plaintiffs and Class Members were customers of Defendant Xfinity, and therefore had entered a contract with Defendant Xfinity.

76. Part of that contract, whether expressed or implied, is that Defendant Xfinity would provide adequate protection of customer's account and person information, and prevent that data from being given away, sold, or stolen.

77. By failing to adequately update their protection software, Defendant has breached their contract with each Plaintiff and Class Member by proving inadequate protection.

78. This breach has resulted in damages and injuries to all Plaintiffs and Class Members, who have had their personal information and account details stolen and thus are more likely to be subject to cyber-attacks, identity fraud, as well as unwanted spam and scam messages.

79. Throughout most of Defendants' history they have provided reasonably proactive data security, preventing many of the cyber-attacks that have targeted Defendants.

80. Defendants' failure to keep and secure the Plaintiffs' and Class Members' data constitutes a material breach of the agreements between Defendant Xfinity and the Plaintiffs and Class Members. By doing so, Defendants have harmed each and every Plaintiff and Class Member.

81. Plaintiffs and the Class seek actual damages, attorney's fees, costs, and any other just and proper relief available thereunder for Defendants' breach of contract.

COUNT III
UNJUST ENRICHMENT
(On Behalf of the Plaintiffs and the Class)

82. Plaintiffs incorporate Paragraphs 1-43 by reference as if fully set forth herein.

83. Plaintiffs and members of the Class have conferred a benefit to Defendants in the form of monies paid for providing services such as home entertainment and internet services, among others.

84. Included in these services provided, whether expressed or implied, is the secured protection and safekeeping of Plaintiffs' and Class Members' personal and account information.

85. These monies were not given as a gift, but rather with the expectation and understanding that services would be provided in return.

86. Defendants have accepted and appreciated the monies paid, as they have continued to provide their services to Plaintiffs and the Class Members, per the terms of their agreements.

87. Then, in the October 2023 Citrix Bleed, Defendants were no longer able to provide safe and secure protection of Plaintiffs' and Class Members' data.

88. This is evident as over 35 million customers' data was unintentionally released in the Citrix Bleed and has been accessed by cybercriminals.

89. Defendants have retained all monies paid by Plaintiffs and Class Members, even though they have failed to provide the secure service that Plaintiffs and Class Members, whether expressed or implied, paid for.

90. Defendants' retention of these monies paid would be inequitable, as the Plaintiffs and Class Members have paid value for a benefit that they were not provided.

91. Not only were the Plaintiffs and Class Members not provided a service for which they paid for, but they will now have to pay additional costs out of pocket in attempts of preventing their data from causing them further harm.

92. Plaintiffs and the Class seek actual damages, attorney's fees, costs, and any other just and proper relief available under the laws.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Class, respectfully request the Court to enter judgment on their behalf and on behalf of the Class as follows:

a) Certification of the action as a Class Action Pursuant to Federal Rule of Civil Procedure 23, and appointment of Plaintiffs as Class Representatives and their counsel of record as Class Counsel;

b) That acts alleged herein be adjudged and decreed to constitute negligence, breach of contract, and unjust enrichment.

c) A judgment against Defendants for the damages sustained by Plaintiffs and the Class defined herein, and for any additional damages, penalties, and other monetary relief provided by applicable law;

d) An order providing injunctive and other equitable relief as necessary to protect the interests of the Class, including, but not limited to:

(1) Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

(2) Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

(3) Ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

(4) Ordering that Defendants segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, unauthorized third parties cannot gain access to other portions of Defendant's systems;

(5) Ordering that Defendants purge, delete, and destroy in a reasonably secure manner consumer data not necessary for their provisions of services;

(6) Ordering that Defendants conducts regular database scanning; and

(7) Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

e) By awarding Plaintiffs and Class Members pre-judgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of the Complaint in this action;

f) The costs of this suit, including reasonable attorney fees; and

g) Such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, individually and on behalf of all those similarly situated, hereby request a jury trial, pursuant to Federal Rule of Civil Procedure 38, on any and all claims so triable.

Dated: January 4, 2024

/s/ Blake G. Abbott
Paul J. Doolittle (Fed ID #6012)
Blake G. Abbott (Fed ID #13354)
POULIN | WILLEY | ANASTOPOULO, LLC
32 Ann Street Charleston, SC 29403
Tel: (803) 222-2222
Email: paul.doolittle@poulinwilley.com
blake.abbott@poulinwilley.com

Attorneys for Plaintiffs